Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December, 2025

Date: 15-12-2025 **Time:** 1.00pm to 04.00pm

School: SOIS	**Program:** BCA	
Course Code: CSA3027	**Course Name:** Cryptography and Network Security	
Semester: V	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**
Marks	**26**	**26**	**24**	**24**

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part - A

Answer ALL the Questions. Each question carries 2marks. 10Q x 2M=20M

1.	Briefly describe the operation of a substitution cipher.	2 Marks	L2	CO1
2.	What is the importance of Feistel structure in cryptography?	2 Marks	L2	CO1
3.	Differentiate between active and passive attacks.	2 Marks	L1	CO1
4.	Briefly describe the role of the S-box in a symmetric cipher like AES.	2 Marks	L2	CO2
5.	What is the significance of the Euclidean Algorithm in cryptography?	2 Marks	L2	CO2
6.	Why is DES considered insecure for modern applications?	2 Marks	L2	CO2
7.	List the three main security requirements for a cryptographic hash function.	2 Marks	L1	CO3
8.	Define a man-in-the-middle attack.	2 Marks	L1	CO3
9.	State two security services provided by PGP.	2 Marks	L1	CO4
10.	Explain the role of a digital certificate in Web Security.	2 Marks	L1	CO4

Part - B

Answer the Questions. **Total Marks: 80M**

11.	**a.**	Explain the three fundamental concepts of the OSI security architecture.	10 Marks	L2	CO1
	b.	Using the principles of the Feistel structure, explain how the encryption and decryption processes have a similar design.	10 Marks	L3	CO1
OR					
12.	**a.**	Explain Caesar cipher with an example. Show encryption and decryption process for the text "HELLO" with key = 3.	10 Marks	L3	CO1
	b.	Discuss the following services with examples: Authentication, Access Control, Data Confidentiality, Data Integrity, and Non-repudiation.	10 Marks	L2	CO1

13.	**a.**	Describe the steps of AES encryption process (SubBytes, ShiftRows, MixColumns, AddRoundKey) in detail.	10 Marks	L2	CO2
	b.	Explain the structure of DES with a neat diagram and describe its working principle.	10 Marks	L2	CO2
OR					
14.	**a.**	Why are prime numbers important in symmetric and asymmetric cryptography? Explain with examples.	10 Marks	L2	CO2
	b.	Discuss the importance of Euclidean Algorithm in number theory and cryptography.	10 Marks	L2	CO2

15.	**a.**	Define a Digital Signature. Explain the process of generating and verifying a digital signature with an example.	10 Marks	L3	CO3
	b.	Describe the RSA algorithm in detail. Illustrate the encryption and decryption process with an example.	10 Marks	L3	CO3
OR					
16.	**a.**	Explain the steps of the Diffie–Hellman Key Exchange protocol. How does it enable two parties to establish a shared secret?	10 Marks	L2	CO3
	b.	Explain Man-in-the-Middle (MITM) attack? Describe, with a clear example, how such an attack is executed against the Diffie-Hellman Key Exchange protocol.	10 Marks	L2	CO3

17.	**a.**	Explain the architecture of IPSec with its components (AH, ESP, Security Associations).	10 Marks	L2	CO4
	b.	Compare and contrast S/MIME and PGP for e-mail security in detail.	10 Marks	L4	CO4
OR					
18.	**a.**	Explain the fundamental security goals of Confidentiality, Integrity, and Availability (CIA Triad). Discuss a relevant mechanism or attack for each.	10 Marks	L2	CO4
	b.	Illustrate different types of security attacks in computer networks with neat diagrams.	10 Marks	L4	CO4